UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	
- v -	:	13 Cr. 761 (VM)
YUDONG ZHU,	:	
Defendant.	:	

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S PRETRIAL MOTION TO SUPPRESS

PREET BHARARA
United States Attorney
Southern District of New York
Attorney for the United States of America

Christian R. Everdell
Assistant United States Attorney
- Of Counsel -

TABLE OF CONTENTS

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum of law in opposition to the defendant's pretrial motion to suppress the evidence seized from his NYU-owned laptop computer. The defendant claims that the Government's search of the laptop computer, which FBI agents conducted after obtaining the consent of NYU, violated his rights under the Fourth Amendment because he had a reasonable expectation of privacy in the contents of the laptop computer and NYU had no actual or apparent authority to consent to the search.

These arguments are meritless and the motion should be denied. First, Dr. Zhu had no reasonable expectation of privacy in the laptop computer. NYU maintains explicit policies concerning employees' use of NYU-owned computers and equipment, which state, among other things, that (i) employees "should not have any expectation of privacy" in NYU computers, e-mail systems, and electronic communications and equipment; (ii) NYU reserves the right to audit and/or examine any NYU-owned computer to ensure compliance with its policies; and (iii) NYU can inspect any of its computers "at any time, with or without cause or notice," and that any attempt by an employee to deny access could lead to discipline or termination. Dr. Zhu signed two different forms when he was hired by NYU in October 2008 in which he specifically acknowledged that he understood these policies. In light if NYU's clear policy of unfettered access to its own equipment, Dr. Zhu cannot create a reasonable expectation of privacy in his NYU-owned laptop computer simply by using encryption software and passwords to hide its contents.

Second, even assuming, *arguendo*, that Dr. Zhu did possess a reasonable expectation of privacy in the contents of the laptop computer, NYU gave valid consent to the FBI to search it. As the owner of the laptop with permission to access it at any time, NYU had actual authority to

consent to the search of its contents. Moreover, at the time the FBI agents obtained NYU's consent, they had an objectively reasonable basis to believe that NYU had the ability to legally consent to the search of the laptop. Accordingly, even if NYU did not have actual authority to consent to the search, the FBI agents appropriately relied on NYU's apparent authority to consent. The defendant's motion therefore should be denied.

RELEVANT FACTS

A. Dr. Zhu's Awareness of NYU Computer Use Policies

New York University Langone Medical Center ("NYULMC") maintains several policies, procedures, and internal regulations that apply to all NYULMC employees. Most of these policies are contained in the Staff Handbook and the Code of Conduct, which are updated from time to time and distributed to all NYULMC employees when they are hired. The Staff Handbook and the Code of Conduct are also available online on the NYULMC intranet, which is accessible to all NYULMC employees, and hard copies are available to any NYULMC employee upon request. (Delts Decl. ¶ 2).

The Staff Handbook contains various policies concerning employees' use of NYULMC equipment, including its communications systems and computer systems. Among other things, the policy on Use of Computer Systems states:

> All staff should know that (1) all electronic communications (e.g., email) are NYU Hospital Center and NYU School of Medicine property; (2) electronic media should be used for business purposes only (other than occasional personal use); and (3) e-mail and internet Website queries communications are automatically stored on a computerized backup system and periodically reviewed.
>
> Computers, e-mail systems, and electronic communications and equipment are the sole property of NYU Hospitals Center and/or NYU School of Medicine, and staff should not have any expectation of privacy. The Hospitals Center and the School of

> Medicine reserve the right to conduct spot audits and/or examinations of any Hospital- or School-owned computer or communications equipment, including those used at home, and all electronic communications sent to or received from such computer or electronic communication equipment for the purpose of ensuring compliance with this and other institutional policies.

(Delts Decl. ¶ 3 & Ex. A at 42). In the section entitled "Lockers, Desks, Personal Computers and Offices," the Staff Handbook further states:

> All lockers, desks, personal computers, and offices remain the property of NYU Medical Center. Accordingly, the Medical Center may inspect a locker, desk, personal computer, or office at any time, with or without cause or notice. Employees who attempt to deny access or to otherwise hinder such investigation are subject to discipline up to and including termination.

(Delts Decl. ¶ 3 & Ex. A at 17).

During the new employee processing, NYULMC distributes to all newly-hired NYULMC employees the Staff Handbook and the Code of Conduct. At that time, they must sign a form acknowledging that they received these items and that they are responsible for reading, understanding, and conforming to the policies and procedures in both handbooks. (Delts Decl. ¶ 4). Also during the new employee processing, newly-hired employees are provided a copy of the Policy Statement on Privacy, Information Security, and Confidentiality. As a condition of employment, all employees must sign this form acknowledging that they understand the contents of this policy, which includes the following statement:

> I understand that the *confidential information* and software I use for my job are not to be used for personal benefit or to benefit another unauthorized institution. I also understand that my institution may inspect the computers it owns, as well as personal PCs used for work, to ensure that its data and software are used according to its policies and procedures.

(Delts Decl. ¶ 5 & Ex. C at 2) (italics in original).

Yudong Zhu was hired by NYULMC as an Assistant Professor in the Department of Radiology in October 2008. On October 20, 2008, Dr. Zhu signed the form acknowledging that received the Staff Handbook and the Code of Conduct and that he was responsible for reading, understanding, and conforming to the policies and procedures in both handbooks. The 2008 version of the Staff Handbook included the same policies concerning Use of Computer Systems and Lockers, Desks, Personal Computers, and Offices as quoted above. (Delts Decl. ¶ 6 & Ex. B). On October 20, 2008, Dr. Zhu also signed the form acknowledging that he understood the Policy Statement on Privacy, Information Security, and Confidentiality, including that NYULMC "may inspect the computers it owns, as well as personal PCs used for work, to ensure that its data and software are used according to its policies and procedures." (Delts Decl. ¶ 7 & Ex. C at 2).

B. NYU's Ownership of the Laptop Computer

In March 2010, NYU applied for and received a research grant from the National Institutes of Health ("NIH") on behalf of Dr. Zhu. (Carna Decl. ¶ 5 & Ex. A at 2). Under the terms of the NIH grant, NYU was to receive a total of nearly $3,000,000, in regular increments, over the time period from February 2011 through January 2015. (Carna Decl. ¶ 6). Each award of grant funds was accompanied by a Notice of Award from NIH, which stated that the grant funds were being awarded to "New York University School of Medicine." (Carna Decl. ¶ 6 & Ex. B). The funds from each of these awards were made available by NIH in a unique account controlled by NYU to reimburse for expenditures related to Dr. Zhu's project that were spent according to the pre-approved budget for his grant project. (Carna Decl. ¶ 6). Among other things, Dr. Zhu used the grant funds to purchase a laptop computer to use for his grant research. (Zhu Decl. ¶ 4). The grant funds, however, remain the property of NYU, and any equipment that

was purchased with grant funds, including the laptop computer that Dr. Zhu now claims was illegally searched, belongs to NYU. (Carna Decl. ¶ 4).

C. NYU Consent to Search the Laptop Computer

On May 19, 2013, this Office filed a two-count criminal complaint charging Dr. Zhu with falsification of records and conspiracy to commit commercial bribery. In connection with that investigation, FBI agents asked NYU to grant consent for the FBI to search the NYU-owned laptop computer used by Dr. Zhu to conduct his grant research, which Dr. Zhu had surrendered to NYU on May 8, 2013. On June 27, 2013, NYU gave consent for the search. (Cline Decl., Ex. 3).

ARGUMENT

I. THE DEFENDANT DOES NOT HAVE A REASONABLE EXPECTATION OF PRIVACY IN THE CONTENTS OF THE LAPTOP COMPUTER

Dr. Zhu's contention that he had a reasonable expectation of privacy in the laptop computer that he purchased with NIH grant funds is meritless. NYULMC maintained policies that explicitly stated that employees should not have an expectation of privacy in any files contained on NYU-owned computers, and that NYULMC reserved the right to inspect and monitor its computers at any time. Dr. Zhu twice signed forms in which he acknowledged that he understood these policies. While Dr. Zhu may have attempted to hide the contents of the laptop computer with encryption and multiple passwords, at best, that indicates that he had a *subjective* expectation of privacy in its contents. In light of NYULMC's clearly articulated computer use policies, however, Dr. Zhu cannot credibly claim that his expectation of privacy was *objectively* reasonable. His Fourth Amendment claim therefore must fail.

A. Applicable Law

When a defendant seeks to suppress evidence by reason of a Fourth Amendment violation, he bears the burden of demonstrating that he has a "legitimate expectation of privacy" in the area searched. *Rakas* v. *Illinois*, 439 U.S. 128, 143 (1978). First, the defendant must show that he had a subjective expectation of privacy in the area searched—in this case, the laptop computer—and second, that his expectation of privacy is one that society accepts as reasonable. *United States* v. *Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008).

In the workplace context, the Supreme Court has recognized that "employees may have a reasonable expectation of privacy against intrusions by police." *O'Connor* v. *Ortega*, 480 U.S. 709, 716 (1987) (citing *Mancusi* v. *DeForte*, 392 U.S. 364 (1968)). However, because office spaces and office equipment are often accessed and used by fellow employees, the "operational realities" of the office can render some employees' expectation of privacy unreasonable. *See O'Connor* v. *Ortega*, 480 U.S. at 717; *see also City of Ontario, Cal.* v. *Quon*, 560 U.S. 746, 756-57 (2010) ("'[O]perational realities' [can] diminish an employee's privacy expectations, and . . . this diminution [can] be taken into consideration when assessing the reasonableness of a workplace search." (citing *Treasury Employees* v. *Von Raab*, 489 U.S. 656, 671 (1989))). For example, an employee's expectation of privacy in his office, desk, and files may be diminished "by an employer's practices procedures, and legitimate regulation over the use of the employer's property." *United States* v. *Bailey*, 272 F. Supp. 822, 835 (D. Neb. 2003) (citing *Ortega*, 480 U.S. at 717). For this reason, employees' expectations of privacy in the workplace must be assessed "on a case-by-case basis." *Ortega*, 480 U.S. at 718.

Since *Ortega*, circuit and district courts have identified several factors that are relevant in determining whether an employee's expectation of privacy in files stored in office computers,

and sent through office computer networks, is objectively reasonable. Chief among these is whether the employer has notified the employees that (i) they have no expectation of privacy in the contents of employer-owned computers and computer systems, and (ii) the employer has the right to monitor or inspect its computers and computer systems. *See, e.g.*, *Leventhal* v. *Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (plaintiff had a reasonable expectation of privacy in his office computer because, *inter alia*, employer had not placed the plaintiff "on notice that he should have no expectation of privacy in the contents of his office computer"); *Muick* v. *Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002) (no reasonable expectation of privacy in laptop computer because the employer "had announced that it could inspect the laptops that it furnished for the use of its employees," which "destroyed any reasonable expectation of privacy that [the plaintiff] might have had and so scotches his claim"); *United States* v. *Angevine*, 281 F.3d 1130, 1134-35 (10th Cir. 2002) (professor had no reasonable expectation of privacy in erased files located on his office computer because university reserved the right to monitor computers connected to the university network); *United States* v. *Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (no reasonable expectation of privacy in Internet use when employer's known policy allowed monitoring of "all file transfers, all websites visited, and all e-mail messages"); *see also United States v. Bailey*, 272 F. Supp. 2d at 836 (no reasonable expectation of privacy in computer files and e-mails where employer notified employees through start-up screen notices and e-mail letters that it could search work computers); *Thygeson* v. *U.S. Bancorp*, No. CV-03-467, 2004 WL 2066746, at *20 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy in computer files and e-mail where employee handbook explicitly warned of employer's right to monitor files and e-mail); *Kelleher* v. *City of Reading*, No. Civ. A. 01–3386, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (no reasonable expectation of privacy in workplace e-mail where employer's

guidelines "explicitly informed employees that there was no such expectation of privacy"); *Garrity* v. *John Hancock Mutual Life Ins. Co.*, No. Civ. A. 00–12143, 2002 WL 974676, at *1-*2 (D. Mass. May 7, 2002) (no reasonable expectation of privacy in work e-mails where employee created a password to limit access, but still knew company could monitor e-mails).

As set forth above, a publicized computer use policy that explicitly disavows the employee's privacy rights and reserves the employer's right to monitor and inspect its computers and computer networks will generally defeat an employee's privacy claim. However, courts may also consider other factors, including whether the employer has established a policy that discourages employees from storing personal files in work computers. *See Leventhal* v. *Knapek*, 266 F.3d at 74 (noting that the employer's policies did not prohibit storing personal files on office computers); *cf. Ortega*, 480 U.S. at 719 (noting that the employer had not "established a [] reasonable regulation or policy discouraging employees . . . from storing personal papers and effects in their desks or file cabinets").[1]

B. Discussion

With respect to the first prong of the analysis, the Government will assume for the purposes of this motion that Dr. Zhu exhibited a subjective expectation of privacy in the laptop computer. Dr. Zhu correctly points out that he encrypted the contents of the laptop and

[1] Several district and bankruptcy courts in this circuit and others have engaged in a similar analysis to evaluate whether an employee can claim a valid attorney-client or spousal privilege for e-mails sent over a company e-mail server. These courts have widely adopted a four-factor test to determine whether the employee has a "reasonable expectation of privacy" in these e-mails: "(1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?" *E.g., In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005). The Second Circuit has not adopted this test, nor is it widely used outside of the privilege context to evaluate Fourth Amendment claims. However, the test is based on the Fourth Amendment case law cited above and leads to the same result in this case. Accordingly, the Government includes it for the Court's reference, but will not rely upon it in its analysis.

established several levels of passwords, which he claims he did not provide to anyone else. (Zhu Decl. ¶ 4). Assuming, *arguendo*, that Dr. Zhu did not share these passwords with third parties, his efforts to exclude others from the contents of the laptop computer are sufficient to establish a subjective expectation of privacy. *See United States* v. *Ziegler*, 474 F.3d 1184, 1189 (9th Cir. 2007); *United States* v. *Slanina*, 283 F.3d 670, 676 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002).

While Dr. Zhu may have had a subjective expectation of privacy in the contents of the laptop computer, his expectation was not objectively reasonable and therefore not protected by the Fourth Amendment. NYULMC maintained clear, well-publicized computer use policies notifying its employees that they had no expectation of privacy in any files or e-mails saved on its computers, and that NYULMC reserved the right to monitor and inspect the contents of its computers and computer networks. For example, NYULMC's policy on Use of Computer Systems, contained in the Staff Handbook, states:

> All staff should know that (1) all electronic communications (e.g., email) are NYU Hospital Center and NYU School of Medicine property; (2) electronic media should be used for business purposes only (other than occasional personal use); and (3) e-mail and internet Website queries communications are automatically stored on a computerized backup system and periodically reviewed.
>
> Computers, e-mail systems, and electronic communications and equipment are the sole property of NYU Hospitals Center and/or NYU School of Medicine, and staff should not have any expectation of privacy. The Hospitals Center and the School of Medicine reserve the right to conduct spot audits and/or examinations of any Hospital- or School-owned computer or communications equipment, including those used at home, and all electronic communications sent to or received from such computer or electronic communication equipment for the purpose of ensuring compliance with this and other institutional policies.

(Delts Decl. ¶ 3 & Ex. A at 42). These same principals are reiterated in the "Lockers, Desks, Personal Computers and Offices" section of the Staff Handbook and in the Policy Statement on Privacy, Information Security, and Confidentiality. (*See* Delts Decl. ¶ 3 & Ex. A at 17 ("[T]he Medical Center may inspect a locker, desk, personal computer, or office at any time, with or without cause or notice."); Delts Decl. ¶ 5 & Ex. C at 2 ("I . . . understand that my institution may inspect the computers it owns, as well as personal PCs used for work, to ensure that its data and software are used according to its policies and procedures.")).

Dr. Zhu was made aware of these policies and signed two separate forms acknowledging that he understood them when he was hired in October 2008. (*See* Delts Decl., Exs. B and C). Hence, Dr. Zhu's claim that he "expected the contents of the laptop would remain private and would not be exposed to anyone within or outside of NYU without [his] consent" rings hollow. (Zhu Decl. ¶ 6). Although Dr. Zhu may have subjectively believed that the contents of the laptop computer would remain private, that belief simply ignored reality and was not objectively reasonable in light NYULMC's clearly expressed policies. *See Muick* v. *Glenayre Electronics*, 280 F.3d at 743; *United States* v. *Angevine*, 281 F.3d at 1134-35; *United States* v. *Simons*, 206 F.3d at 398; *United States v. Bailey*, 272 F. Supp. 2d at 836; *Thygeson* v. *U.S. Bancorp*, 2004 WL 2066746, at *20; *Kelleher* v. *City of Reading*, 2002 WL 1067442, at *8; *Garrity* v. *John Hancock Mutual Life Ins. Co.*, 2002 WL 974676, at *1-*2.

Dr. Zhu argues that his expectation of privacy was objectively reasonable because he took several steps to prevent anyone other than himself from gaining access to the laptop. Specifically, Dr. Zhu points out that "[h]e ordered the laptop and configured it; he protected the laptop with passwords and encryption; he alone had access to it; he did not permit anyone else to use it . . . and he kept it in his possession and control, rather than—for example—leaving it in his

NYU office." (Zhu Mem. at 7). Yet these facts do not alter the critical factor in the analysis, which is that the laptop computer was owned by NYU and, as such, it was subject to NYULMC's policies on computer use. (*See* Carna Decl. ¶ 4; Delts Decl., Ex. A at 42). Dr. Zhu therefore was aware that NYU had the right to access the laptop computer "any time, with or without cause or notice," and that if he attempted to deny NYU access, he could be subject to discipline or even termination. (Delts Decl. ¶ 3 & Ex. A at 17). Dr. Zhu cannot circumvent these policies and establish a reasonable expectation of privacy simply by creating passwords. *See United States v. Bailey*, 272 F. Supp. 2d at 836 (password protection did not create reasonable expectation of privacy in files on work computer where employer notified employees that it could search work computers); *Garrity* v. *John Hancock Mutual Life Ins. Co.*, 2002 WL 974676, at *1-*2 (no reasonable expectation of privacy in work e-mails where employee created a password to limit access, but still knew company could monitor e-mails).

The cases cited by Dr. Zhu that address password protection—*United States* v. *Slanina*, 283 F.3d 670 (5th Cir. 2002); *United States* v. *Reeves*, 2012 U.S. Dist. LEXIS 68962 (D.N.J. May 17, 2012); *United States* v. *Howe*, 2011 U.S. Dist. LEXIS 57491 (W.D.N.Y. May 27, 2011); and *United States* v. *Robson*, 2007 U.S. Dist. LEXIS 53627 (E.D. Mich. July 24, 2007)—are easily distinguished and do not support the conclusion that Dr. Zhu's use of passwords created a reasonable expectation of privacy in the contents of his NYU-owned laptop. In each of these cases, the court found that the computer user had a reasonable expectation of privacy in the contents of the computer, in part, because the computer was password-protected. However, *none* of these cases involved a situation where, as here, the employer had notified the employee that he had no reasonable expectation of privacy in the contents of the computer and that the employer could inspect or monitor the computer at any time. *See Slanina*, 283 F.3d at 676-77; *Reeves*,

2012 U.S. Dist. LEXIS 68962 at *20-*24; *Howe*, 2011 U.S. Dist. LEXIS 57491, *17-*20; and *Robson*, 2007 U.S. Dist. LEXIS 53627, at *10-*13. Indeed, only *Slanina* and *Reeves* involved the search of an employee's work computer—*Howe* and *Robson* involved searches of personal computers—and *Slanina* specifically noted the lack of a policy alerting employees that the employer could monitor computer use in reaching its finding. *See Slanina*, 283 F.3d at 677 ("[G]iven the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable."). Accordingly, these cases are inapposite.

Nor does the Second Circuit's opinion in *Leventhal* v. *Knapek*, 266 F.3d 64 (2d Cir. 2001), which Dr. Zhu discusses at length in his memorandum, support his argument for suppression. Although the *Leventhal* Court found that the plaintiff had a reasonable expectation of privacy in the contents of his employer-owned laptop computer, the Court specifically noted, as the Fifth Circuit later did in *Slanina*, that the employer did not have "a general practice of routinely conducting searches of office computers," nor had the employer "placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer." *Leventhal*, 266 F.3d at 74 (citing *United States* v. *Simons*, 206 F.3d at 398). Instead, the employer had a rather weak anti-theft policy, which did not prohibit the storage of personal materials on office computers. In addition, although the employer's technical staff had access to the work computers to provide technical support and maintenance, they accessed the computers infrequently and almost always announced when they did so. Under these circumstances, the Court found that the employee had a reasonable expectation of privacy in his work computer. *See id.*

Dr. Zhu argues that his situation is akin to Leventhal's because NYULMC did not have "a general practice of routinely conducting searches of office computers" and NYULMC's policies did not categorically forbid employees from storing personal data on work computers. (*See* Zhu Mem. 8-10). In support of this argument, Dr. Zhu claims that, to his knowledge, NYU had never requested access to computers used by other NYU professors. (*See* Zhu Decl. ¶ 9). Even assuming the truth of this assertion, it is beside the point. As *Leventhal* makes clear, it is sufficient if an employer places its employees on notice, as NYULMC did, that they should not have any expectation of privacy in their work computers because the computers can be monitored. It is not necessary for the employer also to regularly search their computers to eliminate the employees' reasonable expectation of privacy. *See Leventhal*, 266 F.3d at 74 ("[W]e do not find that [the employer] had a general practice of routinely conducting searches of office computers *or* had placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer." (emphasis added)). Similarly, although NYULMC's policies allowed for "occasional personal use" of work computers (Delts Decl., Ex. A at 41), that one fact does not negate its clearly communicated message that employees have no reasonable expectation of privacy in any of the files they place on NYU-owned computers, personal or otherwise. The cases cited by Dr. Zhu do not suggest otherwise because they did not involve such a policy. *See Leventhal*, 266 F.3d at 74l; *Slanina*, 283 F.3d at 676-76); *Convertino* v. *Dept. of Justice*, 674 F. Supp. 2d 97, 110 (D.D.C. 2009).

In sum, Dr. Zhu was on notice that his NYU-owned laptop computer could be accessed, monitored, or inspected at any time, and that he should have no expectation of privacy in any of its contents. Accordingly, he has no basis to challenge the search and his motion to suppress should be denied.

II. NYU GAVE VALID CONSENT TO SEARCH THE COMPUTER

Even assuming, *arguendo*, that Dr. Zhu had a reasonable expectation of privacy in the contents of his laptop computer, the FBI's search of the laptop did not violate the Fourth Amendment because NYU gave valid consent for the search. Contrary to Dr. Zhu's assertions, NYU had the authority to permit the search because it owned the computer and had the right to access it any time, despite the passwords and encryption that Dr. Zhu placed on it. Alternatively, based on what the FBI agents knew about NYU's control over the computer at the time of the search, they appropriately relied on NYU's apparent authority to consent. Accordingly, Dr. Zhu's motion to suppress should be denied.

A. Applicable Law

The Fourth Amendment "generally requires police to secure a warrant before conducting a search." *Maryland* v. *Dyson*, 527 U.S. 465, 466 (1999) (*per curiam*). Searches "conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." *Katz* v. *United States*, 389 U.S. 347, 357 (1967). One of the well-established exceptions is a search that is conducted pursuant to consent. *See Schneckloth* v. *Bustamonte*, 412 U.S. 218, 219 (1973). Where the Government seeks to justify a search based on consent, the Government bears the burden of proving by a preponderance of the evidence that the consent was valid. *See United States* v. *Matlock*, 415 U.S. 164, 177 n.14 (1974); *United States* v. *Snype*, 441 F.3d 119, 130-31 (2d Cir. 2006).

Consent may be given by a third party "who possess[es] common authority over or other sufficient relationship to the premises or effects sought to be inspected." *United States* v. *Matlock*, 415 U.S. at 170-71. The Second Circuit has articulated a two-part test for third party

consent that elaborates on the holding of *Matlock*: a third party has the authority to consent where that person "(1) has access to the area searched and (2) has either (a) common authority over the area, (b) a substantial interest in the area, or (c) permission to gain access to the area." *Moore* v. *Andreno* 505 F.3d 203, 209 (2d Cir. 2007) (citing *United States* v. *Davis*, 967 F.3d 84, 87 (2d Cir. 1992). At its root, *Matlock* "stands for the proposition that the reasonableness of . . . a [third-party consent] search is in significant part a function of commonly held understanding about the authority that co-inhabitants may exercise in ways that affect each other's interests." *Georgia* v. *Randolph*, 547 U.S. 103, 111 (2006).

"[E]ven if a third party lacks actual authority to consent to a search of a particular area, he may still have apparent authority to consent to the search." *Moore*, 505 F.3d at 209. If a law enforcement officer has an objectively reasonable belief that he obtained valid consent to search, even if that belief is incorrect, the search does not violate the Fourth Amendment. *Id*. (citing *Illinois* v. *Rodriguez*, 497 U.S. 177, 188 (1990)). The critical inquiry is whether "the facts available to the officer at the moment . . . [would] warrant a man of reasonable caution in the belief that the consenting party had authority over the premises." *Illinois* v. *Rodriguez*, 497 U.S. at 188 (internal quotation marks omitted).

B. Discussion

Dr. Zhu first asserts that the Government cannot satisfy the first prong of the *Davis* test, because NYU did not have "access" to the laptop due to the encryption and passwords that he placed on it. This argument elevates form over substance. Although the Second Circuit has never defined the term "access," it has never held "that access must mean *physical* access and not legal access." *Ehrlich* v. *Town of Glastonbury*, 348 F.3d 48, 60 (2d Cir. 2003); *accord* *Moore*, 505 F.3d at 210. In *Ehrlich*, the conservator of the plaintiff's estate provided consent to

various people to enter the plaintiff's home by "whatever means necessary" to retrieve the plaintiff's personal items, which they did by forcing entry into the residence. *Id*. at 50. The Second Circuit found that "access" requirement of the *Davis* test did not necessarily preclude the use of force to gain access to the premises as long as the third party giving the consent had legal access. *Id*. at 60. In discussing the *Davis* test, which the *Ehrlich* Court called an "elaboration" on Supreme Court precedent, the Court noted that "the Supreme Court has never identified 'access' as a prerequisite to a valid consent to search," and that *Matlock* itself "did not differentiate between access and authority." *Id*. at 60 & n.17.

Here, NYU most certainly had legal access to the laptop. First, NYU owned the laptop because it was purchased with NIH grant funds. (*See* Carna Decl. ¶ 4; Zhu Decl. ¶ 4). Second, according to its policies, NYU reserved the right to inspect the computer "at any time, with or without cause or notice." (Delts Decl. ¶ 3 & Ex. A at 17). Third, Dr. Zhu consented to NYU's unlimited access to the laptop by signing the form when he was hired acknowledging that he understood this policy. (Delts Decl., Ex. B). Fourth, Dr. Zhu was aware that if he tried to deny NYU access to the laptop, as he did by installing encryption and passwords, he would be subject to termination. (Delts Decl. ¶ 3 & Ex. A at 17).

Accordingly, Dr. Zhu's laptop is not like the password-protected laptop in *United States* v. *Griswold*, 2011 U.S. Dist. LEXIS 153943 (W.D.N.Y. June 2, 2011), as he claims. In *Griswold*, the court held that while the defendant's mother had the right to retrieve her son's password-protected laptop from his room and deliver it to law enforcement agents, she did not have actual authority to consent to search it. *Griswold*, 2011 U.S. Dist. LEXIS 153943, at *11-*13. The mother in *Griswold*, however, did not have the son's written acknowledgement that she could inspect his laptop at any time. NYU had such an acknowledgement from Dr. Zhu,

which provided NYU unquestioned legal access to the laptop. (Delts Decl., Ex. B). *Griswold* is therefore inapposite.

For the same reasons, the Government can also satisfy the second prong of the *Davis* test because NYU had (1) common authority over, (2) a substantial interest in, and (3) permission to gain access to the laptop computer. As an initial matter, it cannot seriously be disputed that NYU owns the laptop computer that was searched by the FBI. Dr. Zhu concedes that he bought the computer with NIH grants funds, and does not argue that he was the owner of the computer. (*See* Zhu Decl. ¶ 4). However, he also states that "NYU did not pay for [the computer]," insinuating that NYU does not own it either. (Zhu Mem. at 13). This suggestion is directly rebutted by NYU's factual proffer that it owns any equipment that is purchased with NIH grant funds. (*See* Carna Decl. ¶ 4). NYU's ownership of the computer, combined with its ability to gain access to it at any time and Dr. Zhu's written acknowledgement and consent that access, establishes all three sub-prongs of the second *Davis* factor. *See United States* v. *Ziegler*, 474 F.3d at 1191-92 (employer had common authority over defendant's workplace computer because employer "had complete administrative access" to all work computers and notified its employees that the computers were company-owned and regularly monitored); *Davis*, 967 F.2d at 87 (third party's "ownership and actual possession of the trunk . . . coupled with his ready access to it" established common authority and substantial interest); *Matlock*, 415 U.S. at 171 n.7 (common authority exists when "it is reasonable to recognize [the consenting party] has the right to permit the inspection in his own right and that [the defendant has] assumed the risk that [the consenting party] might permit the common area to be searched").

That NYU did not know the passwords is of no consequence and, contrary to Dr. Zhu's assertions, does not eliminate NYU's common authority or substantial interest in the laptop. The

cases that Dr. Zhu cites in support of this point are, once again, inapposite. In *United States* v. *Buckner*, 473 F.3d 551 (4th Cir. 2007), the court found that the defendant's wife did not have common authority over a computer that her husband had password-protected and therefore did not have actual authority to consent to the search. *Id*. at 554. Similarly, in *Trulock* v. *Freeh*, 275 F.3d 391 (4th Cir. 2001), the court found that the plaintiff's live-in girlfriend could not consent to the search of the plaintiff's password-protected files contained within a jointly used computer, because she did not know the password. *Id*. at 403. Unlike this case, however, neither *Buckner* nor *Trulock* involved a written acknowledgement by the computer user that a third party could access the computer at any time. (Delts Decl., Ex. B). This acknowledgement not only preserves NYU's common authority over the laptop, it also functions as a grant of permission to NYU to access the laptop, which the password-protection cannot defeat. Accordingly, NYU had actual authority to consent to the search of the laptop.[2]

Even assuming that NYU did not have actual authority to consent to the search, which it did, the FBI agents had an objectively reasonable belief that NYU had the authority to consent, and properly relied on NYU's apparent authority. *See Moore*, 505 F.3d at 209 (citing *Illinois* v. *Rodriguez*, 497 U.S. at 188). Here, the FBI agents knew that the computer belonged to NYU and that it was used by Dr. Zhu to conduct his research at NYU. This was substantiated by the fact that Dr. Zhu had surrendered the computer to NYU in May 2013 at NYU's request. (Zhu Decl. ¶ 7). It was therefore reasonable for the FBI to believe that NYU could consent to the search

[2] In a footnote, Dr. Zhu also cites *United States* v. *Sims*, 2001 U.S. Dist. LEXIS 25819 (D.N.M. 2001) to argue that even if NYU had actual authority to search the laptop itself, they lacked the authority to consent to a search of the laptop by law enforcement. (*See* Zhu Mem. at 14 n. 2). In *Sims*, the Government argued on appeal that the district court's decision was incorrect in light of the Tenth Circuit's subsequent decision in *United States* v. *Angevine*, 281 F.3d 1130 (10th Cir. 2002). The Tenth Circuit declined to rule on the issue, but at least one district court has noted that *Sims* is an outlier case that may no longer be good law in the Tenth Circuit and is inconsistent with the law in the Fourth Circuit. *See United States* v. *Bode*, No. ELH–12–158, 2013 WL 4501303, at *18-*20 (D. Md. Aug. 21, 2013).

despite the passwords and encryption that Dr. Zhu placed on the computer. *See Buckner*, 473 F.3d at 555 (agents had reasonable belief that wife could consent to search of password-protected computer used by husband because, among other things, the computer was leased solely in her name and she could return the computer to the rental agency at any time without husband's consent).

Dr. Zhu cites a number of cases in which courts found that third parties did not, or may not have had apparent authority to consent to the search of a laptop because they did not know the password. *See United States* v. *Cole*, 2008 U.S. Dist. LEXIS 57437 (D. Me. July 24, 2008); *Griswold*, 2011 U.S. Dist. LEXIS 153943; *Robeson*, 2007 U.S. Dist. LEXIS 53627. Yet none of these cases involved employers consenting to the search of employer-owned laptops. Rather, these cases involved searches of personal computers located in homes and that were consented to by family members or partners. *See Cole*, 2008 U.S. Dist. LEXIS 57437, at *13-*15; *Griswold*, 2011 U.S. Dist. LEXIS 153943, at *13-*19; *Robeson*, 2007 U.S. Dist. LEXIS 53627, at *18-*19. It was reasonable for the FBI agents to believe that passwords and encryption placed on a work computer would not compromise the employer's right to grant access to its own equipment. Moreover, even if the FBI agents had asked NYU for further clarification on their right of access when they discovered the passwords and encryption on the laptop, as Dr. Zhu claims they should have done, they would have been shown the Staff Handbook, which unequivocally gives NYU unfettered access to its computers. Accordingly, the agents could rely on NYU's apparent authority to consent to the search of Dr. Zhu's laptop.

CONCLUSION

For the foregoing reasons, the Court should deny the defendant's pretrial motion to suppress the evidence seized from the laptop computer.

Dated: New York, New York
April 11, 2014

Respectfully submitted,

PREET BHARARA
United States Attorney

By: _____/s/_____
Christian R. Everdell
Assistant United States Attorney
(212) 637-2556

CERTIFICATE OF SERVICE

I, Christian R. Everdell, Assistant United States Attorney for the Southern District of New York, hereby certify that on April 11, 2014, I caused a copy of the Government's Memorandum of Law in Opposition to Defendant's Pretrial Motion to Suppress to be filed on ECF and thereby to be delivered by electronic mail to the defendant's counsel at the following addresses:

John D. Cline, Esq.
Law Office of John D. Cline
235 Montgomery Street, Suite 1070
San Francisco, CA 94104
cline@johndclinelaw.com

Maurice Sercarz, Esq.
Sercarz & Riopelle, LLP
810 Seventh Avenue, Suite 620
New York, NY 10019
msercarz@sercarzandriopelle.com

Dated: New York, New York
April 11, 2014

_____/s/_____
Christian R. Everdell
Assistant United States Attorney
(212) 637-2556